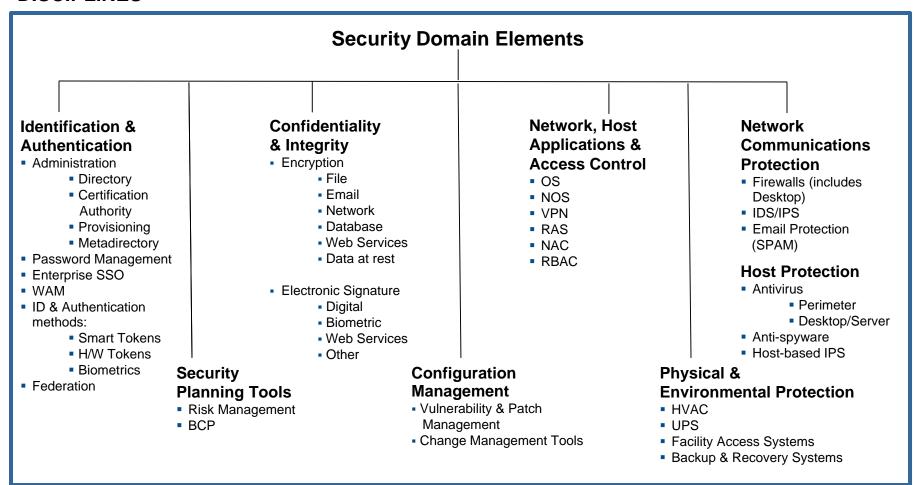
## **Security Domain Profile**

## **DISCIPLINES**



#### **DOMAIN STRATEGY**

Provide a standards based security framework that supports a statewide policy to ensure the confidentiality, integrity and availability of information and information systems.

# **Security Domain Profile (Cont'd)**

### DOMAIN PRINCIPLES/BOUNDARIES

- Confidentiality: "Providing authorization and restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information"
  - Develop and implement security policies and technologies to maintain confidentiality of constituent and employee information.
- Integrity: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity"
  - Develop a secure, robust IT infrastructure capable of initiating, confirming and executing all manner of business transactions.
  - □ Implement a data security architecture that will provide a secure mechanism for data acquisition, storage, retrieval and update.
  - Maintain sufficient computer forensic information and technology to combat specific threats and to investigate and prosecute specific criminal acts.
- Availability: "Ensuring timely and reliable access to or use of information or an information system."
  - Maintain sufficient backup and disaster recovery expertise to minimize the effect of catastrophic events on the information technology infrastructure.
  - □ Promote business continuity plans to ensure reliable and secure service delivery.
- Select products based on industry standards, TCO, and data integrity.
- Favor products that use existing skill sets and/or that are readily available in the market.
- Choose products from viable vendors that have good to excellent support and venders judged to be viable for the future.
- Avoid leading edge or unproven technologies unless there is significant reward.